УДК 681.326

В.Г. КОТУХ, канд. техн. наук, М.А. МИРОШНИК, канд. техн. наук,
С.Н. СЕЛЕВКО, канд. техн. наук

ОТКАЗОУСТОЙЧИВОСТЬ РАСПРЕДЕЛЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Введение

Возрастание сложности современных телекоммуникационных систем влечет за собой необходимость решения задач обеспечения требуемого уровня отказоустойчивости, надежности, робастности, производительности и быстрой адаптации к классу решаемых задач. Надежность, в общем случае, вероятность того, что система будет функционировать надлежащим образом в течение определенного промежутка времени. Надежность сети связи характеризует ее свойство обеспечить связь, сохраняя во времени значения установленных показателей качества в заданных условиях эксплуатации. Она отражает способность сохранять работоспособность сети связи при воздействии случайных отказов технических средств, вызываемых процессами старения, дефектами технологии изготовления или ошибками обслуживающего персонала.

Одним из эффективных путей достижения высоких показателей надежности телекоммуникационных систем является введение аппаратной, программной и временной избыточности, обеспечивающей их отказоустойчивость (свойство системы сохранять работоспособность при наличии в ней неисправностей определенного класса [1]).

Отказоустойчивость телекоммуникационной системы обеспечивается ее внутренними ресурсами путем использования аппаратно-программных средств диагностирования технического состояния и восстановления работоспособности системы при наличии отказов, дефектов обусловленных типов и кратности [2].

Системы распределенной обработки, или распределенные системы (РС), функционирующие в компьютерных сетях, являются одной из наиболее перспективных и быстро развивающихся областей информатики [1]. Такое место они заняли благодаря их существенным преимуществам по сравнению с изолированными системами, функционирующими на базе отдельных компьютеров. РС характеризуются потенциально более высокой надежностью, гибкостью использования вследствие представления пользователю широкого спектра информационных и вычислительных услуг, высокой степенью параллелизма обработки данных, то есть высокой производительностью. Однако достижение отмеченных достоинств сопряжено с решением комплекса проблем, связанных со значительным усложнением механизмов управления информационными процессами, особенно при децентрализации последнего. При этом особое значение имеет обеспечение целостности и не противоречивости распределенных баз данных (РБД) – одного из основных функциональных компонентов РС [2].

Примем следующую модель РС, реализующую транзактную обработку. В множестве узлов $S=\{\frac{S_i}{i}=\overline{1,n}\}$ в каждый момент времени функционируют два подмножества:

$\{TM_i\}$ – подмножество узлов, инициирующих работы (транзакции);

$\{DM^k\}$ – подмножество узлов, выполняющих (обрабатывающих) транзакции.

Такое разделение соответствует разделению работы компьютеров в режиме client-server. При этом $\{TM_i\}\subseteq S$, $\{DM^k\}\subseteq S$, $\{TM_i\}\cap\{DM^k\}\neq\varnothing$.

Здесь последняя строка означает, что один и тот же узел может одновременно инициировать и выполнять транзакции. По завершении обработки транзакций и при появлении новых эти подмножества в общем случае изменяют свой состав.

Транзакции, инициированные узлом TM_i, будем обозначать T_i. В общем случае T_i выполняется в нескольких узлах DM^k. Ту часть T_i, которая выполняется в одном узле DM^k,

будем называть подтранзакцией и обозначать T_i^k. Будем отождествлять транзакцию с множеством составляющих ее подтранзакций: $T_i = \{T_i^1, ..., T_i^{n_i}\}$.

Каждая подтранзакция T_i^k перед началом своей работы должна захватить в узле DM^k локальную базу данных (ЛБД), которую будем называть информационным ресурсом данного узла, или просто ресурсом. Если $\{DM_i^k\} \cap \{DM_j^k\} = \varnothing$, то транзакции T_i и T_j не конфликтуют. Если $\{DM_i^k\} \cap \{DM_j^k\} \neq \varnothing$, то транзакции называются конфликтующими (конкурирующими) за ресурс узла DM^k. Во многих работах допускается функционирование в одном узле DM^k нескольких ЛБД.

Основные понятия отказоустойчивости

Процесс функционирования каждой системы можно рассматривать как последовательность переходов из одного состояния в другое. Возможны переходы, приводящие к ошибочным состояниям, при которых проявляется неисправность.

Существует два типа неисправностей: физические (объективные) и нефизические (субъективные). Неисправности первого типа возникают вследствие внезапного изменения параметров аппаратуры системы и выхода их за допустимые пределы, что вызывает непредусмотренные изменения одной или нескольких числовых и/или логических переменных, используемых в вычислениях. Если изменения носят временный характер, то их называют сбоями, если же эти изменения постоянны, то – отказами. Отказы вызывают неисправность и имеют характер необратимого механического или иного разрушения аппаратуры. Сбои обусловлены временными неблагоприятными воздействиями окружающей среды на электронную аппаратуру. Они приводят к разовому искажению информации, обрабатываемой или хранимой в устройствах, подвергшихся данному воздействию. Неисправности второго типа связаны:

·- с недостатками программного обеспечения системы, которые оставались не выявленными вплоть до момента обнаружения ошибки;

- неустраненными недостатками аппаратуры, которые являются следствием проектных недоработок конструкции, монтажа и последующих модификаций;

- неправильным взаимодействием человека-оператора с машиной и т.д. Такие неисправности вызваны не физическими явлениями, они происходят вследствие субъективных ошибок, допущенных людьми в ходе создания и эксплуатации системы обработки информации.

Возникновение как объективных, так и субъективных неисправностей, как правило, вызывает ошибку. Ошибкой системы принято называть отклонение ее поведения как логической машины от последовательности состояний, заданных программой, и переход к последовательности ошибочных состояний. Ошибка в системе оказывает влияние на процесс функционирования, вследствие чего возникает отказ. Таким образом, ошибка представляет собой проявление неисправности в системе, а отказ – это эффект влияния ошибки на процесс функционирования. Следовательно, причинами нарушений нормального функционирования системы являются объективные и субъективные неисправности. Именно они приводят систему в ошибочное состояние, при котором система не может правильно выполнять функции обработки информации. Простым путем выхода из ошибочного состояния является проведение технического обслуживания и ручного ремонта, что приводит к устранению причин неисправности. Затем система запускается вновь и работает до возникновения следующей неисправности или до запланированного профилактического ремонта.

Задача обеспечения надежности включает определение тех классов неисправностей, по отношению к которым должна быть обеспечена устойчивость, т.е. следует создавать такие системы, которые автоматически обнаруживают и идентифицируют отказы, устраняют их и продолжают нормальную работу.

В последнее время в рамках общей проблемы надежности возникло новое направление – отказоустойчивость системы. В связи с расширением потребности в отказоустойчивых систем и значительным снижением стоимости электронных компонентов в ближайшем будущем ожидается, что подобные системы найдут широкое применение. Для обеспечения эффективного функционирования систем необходима их полная устойчивость к небольшим отказам. При этом допускается некоторое уменьшение производительности системы.

Введение свойства отказоустойчивости позволяет несколько иначе подойти к решению проблемы неисправностей, возложив на саму систему функции устранения их влияния и восстановления нормального функционирования. Можно сказать, что отказоустойчивость обеспечивает жизнеспособность системы, так как ее задачей является возвращение из ошибочного состояния к регулярному состоянию системы, что обеспечивает возможность практически стопроцентного правильного функционирования.

Отказоустойчивость – одна из надежностных характеристик компьютерных систем, отражающая способность выполнять возложенные на систему функции (быть может, не в полной мере) при отказах аппаратных средств.

При рассмотрении отказоустойчивости принимается, что основные характеристики надежности аппаратных средств заданы и рассматривают только негативные последствия сбоев и отказов аппаратных средств на функционирование системы и методы минимизации влияния этих последствий на выполнение основных функциональных задач. С этой точки зрения целесообразно было бы вместо термина "отказоустойчивость" применять термин "функциональная устойчивость системы к отказам". Это подчеркивало бы тот факт, что для полной характеристики системы недостаточно знать коэффициенты готовности отдельных компонент аппаратных средств, но необходимо учитывать, как деградируют функции компьютерной системы за время отказа этих компонент и как деградация отдельных функций влияет на основную функциональную задачу системы.

Наиболее характерными классами компьютерных систем, для которых ведутся интенсивные поисковые исследования и инженерные разработки с целью повышения их отказоустойчивости, являются системы управления техническими и технологическими объектами, а также системы массового сервиса, как правило, реализующие транзактную технологию.

Для систем управления, как правило, удается ввести функцию убытка (штрафа), отражающую степень ухудшения управления в зависимости от времени простоя компьютерной системы. Хороший пример такого подхода содержится в [3-4]. Функция убытка монотонно возрастает во времени. Существуют системы, и их немало, характерные тем, что прекращение решений одной из функциональных задач на некоторое время, большее T, может привести к непоправимым последствиям, делающим дальнейшее функционирование системы бессмысленным. Такие системы получили название систем с жесткой средой реального времени [5]. В таких системах управление носит дискретный (скачкообразный) характер: если система осуществляет управление за T, то штраф отсутствует, если же не осуществляет (из-за отказа любой компоненты компьютерной системы), то штраф максимален.

В системах с транзактной обработкой в качестве функции убытка также рассматривается дискретная функция, характеризующая факт нарушения или ненарушения целостности РБД. Такая постановка вопроса, с одной стороны, является в настоящее время особенно актуальной в связи со всеобщей компьютеризацией общества и катастрофическими последствиями нарушения целостности больших РБД, а с другой стороны, делает более оправданным применение термина "отказоустойчивость", а не "функциональная устойчивость".

Свойством отказоустойчивости обладают многие технические системы, но компьютерные являются в данном случае наиболее характерными, так как они способны адаптироваться к изменяющимся условиям, т.е. перестраивать алгоритмы своего функционирования в широком диапазоне. Среди компьютерных систем свойство отказоустойчивости в наибольшей степени присуще, во всяком случае, потенциально, распределенным системам, функционирующим на основе компьютерной сети [6]. Мало того, можно утверждать, что полез-

ное функционирование распределенных системы, не обладающей свойством отказоустойчивости (или обладающей этим свойством в малой степени), попросту невозможно.

Службу отказоустойчивости представим как иерархическую систему, состоящую из следующих уровней:

– виртуального кольца;
– службы слежения;
– управления фиксацией транзакций;
– резервирования файлов.

В данной работе рассматривается уровень управления резервированными данными. Резервирование данных на уровне различных информационных объектов, например файлов, отношений реляционных БД (или их частей), применяется для достижения двух целей.

Во-первых, для приближения информации к пользователю. Тогда узлы будут быстрее реагировать на поступающие сообщения, а значит, будет быстрее функционировать вся РС.

Во-вторых, для повышения отказоустойчивости РБД, т.е. при отказе некоторого узла можно использовать копии данных, хранящихся в этом узле, но размещенные в других (функционирующих) узлах. Таким образом, обеспечивается высокая степень доступности данных, минимизируется влияние отказов узлов.

Обе эти цели не противоречат друг другу, но тем не менее в ряде случаев требуют различных механизмов работы с резервированными данными.

Ниже рассматривается алгоритм управления резервированными данными, обеспечивающий отказоустойчивость распределенной системы.

Алгоритм.

Шаг 1. Для каждого зарезервированного информационного объекта одна из копий объявляется основной. Транзакция инициируется и выполняется только с основной копией.

Шаг 2. После обработки транзакции, список проведенных изменений рассылается в узлы со вторичными копиями.

Шаг 3. Узлы со вторичными копиями получив список изменений выполняют и посылают узлу с основной копией подтверждение о выполнении действий.

Шаг 4. Если обнаружен отказ узла со вторичной копией, узел с основной копией запоминает список изменений в стабильной памяти и досылает его после восстановления узла со вторичной копией. При этом:

а) узел с основной копией начинает следить за восстановлением узла;

б) вписывает соответствующую запись в таблицу, которая содержит номер узла, вышедшего из строя, указатель на список изменений, номер версии, который должен быть сохранен.

Шаг 5. Как только узел со вторичной копией восстанавливается, он сообщает номер своей версии основной копии, и все задержанные списки изменения будут доставлены.

Шаг 6. Узлы со вторичными копиями как только получают уведомление, что узел с основной копией отказал, подмножество узлов, хранящих вторичные копии, выбирают новую основную копию, не дожидаясь восстановления указанного узла.

Шаг 7. После восстановления бывший узел основной копии посылает широковещательный запрос внутри указанного подмножества и выясняет, где теперь хранится основная копия, просит прислать ему список изменений и начинает функционировать уже в качестве узла, хранящего вторичную копию.

Для обоснования корректности данного алгоритма следует сделать два замечания. Во-первых, все узлы со вторичной копией имеют одну и ту же версию информационного объекта. Во-вторых, здесь не рассматривается возможность фрагментации сети.

Заключение

Таким образом, в работе рассматривается одна из проблем создания распределенных систем – проблема обеспечения отказоустойчивости системы. Приводится модель распределенной системы, реализующая транзактную обработку. Рассматриваются основные понятия

отказоустойчивости. Предлагается алгоритм управления резервированными данными, обеспечивающий отказоустойчивость распределенной системы.

Список литературы: 1. *Фатуллаев, Р.Э.* Отказоустойчивость распределенных систем // Информационные технологии моделирования и управления. – 2006. – №6(31). 2. *Мирошник, М.А., Котух, В.Г.* Разработка методов повышения отказоустойчивости и надежности функционирования компонентов телекоммуникационных систем и сетей // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 164. – С. 190–197., 3. *Ozsu, M.T., Valduries, P.* Principles of Distributed Database Systems, Prentice-Hall, 1999. 4. *Krishna, C.M., Shin, K.G., Lee, Y.H.* Optimization criteria for checkpoint placement // Comm.ACM. – 1984. – 27. – N10. – P.1008-1012. 5. *Leinbaugh, D.W., Yament, M.R.* Guaranteed response times in a distributed hard-realtime environment // IEEE Trans. of Software Eng. – 1986. – 12. – N12. – P.1139-1144. 6. *Flavin Cristan* Understanding Fault-Tolerant Distributed Systems // Comm.ACM.– 1991 – 43, N2. – P. 56-78.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 25.02.2012